RISK ASSESSMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC Risk Management Policy and Procedures							
Effective Date:		01/01/2021		**Document Owner:**		NextGen CGI, LLC	
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy/Proc	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Purpose

All activities undertaken by NextGen CGI, LLC carry an element of risk. Awareness of these risks is critical to understanding, analyzing, and managing functions that carry risk. This policy provides the NextGen CGI risk assessment policy statements and outlines the NextGen CGI's guidelines in developing, implementing, and maintaining a successful risk assessment process.

2. Scope

This policy applies to all company officers, directors, IT specialists, employees, agents, affiliates, contractors, consultants, advisors or service providers that are involved in the risk management process at NextGen CGI. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it.

3. Risk Assessment Controls

- General Risk Assessment
- Vulnerability Scanning
  - Organizational Systems
  - Applications
- Vulnerability Remediation

4. Risk Assessment Methodology

The methodology adopted by NextGen CGI for assessing risks can be defined as follows:

- NextGen CGI will scan for vulnerabilities in organizational systems and applications on a daily basis, or hourly in some cases.
- NextGen CGI will ensure that vulnerabilities are remediated in accordance with risk assessments

4.1 Risk Assessment Matrix

Risk Assessment Matrix

Likelihood Rating	Minor	Serious	Severe	Major	Catastrophic
5. Almost Certain	Medium	High	Critical	Critical	Critical
4. Likely	Medium	Significant	High	Critical	Critical
3. Possible	Medium	Medium	Significant	High	Critical
2. Unlikely	Low	Low	Medium	Significant	Critical
1. Rare	Low	Low	Medium	Medium	High

LIKELIHOOD

CONSEQUENCE

Critical	Extreme risk - detailed research and management planning required at senior levels
High	High risk- immediate senior management attention needed
Significant	Significant risk - Senior management attention needed
Medium	Moderate risk - Management responsibility must be specified
Low	Low risk - Manage by routine procedures

4.2 Risk Consequence Severity

Consequence Type	Minor	Serious	Severe	Major	Catastrophic
Financial Loss	<$1M	$1M-5M	$5M-10M	>$10M	Threatens Viability of Company
Reputational Loss					

4.3 Likelihood Probability and Frequency

Likelihood Rating	Description	Probability
Almost Certain	Known to happen often	>95%
Likely	Could easily happen	50-95%
Possible	Could happen & has occurred in the past	15-50%
Unlikely	Hasn't happened yet but could	5-15%
Rare	Conceivable, but only in extreme circumstances	>5%

4.4 Control Effectiveness

Control Effectiveness	Description
Effective	The control design meets the control objective and the control is operating the majority of the time
Partially Effective	The control design mostly meets the control objective and/or the control is normally operational but occasionally is not applied when it should be, or not as intended
Ineffective	The control design does not meet the control objective and/or the control is not applied or is applied

4.5 Risk Register

No	Risk	Owner	Consequence	Likelihood	Inherent Risk Level	Controls	Control Effectiveness
1							
2							
3							
4							

5. Related Standards, Policies, and Processes

- Threat and Risk Assessment Procedures
- Security Assessment Procedures
- Plan of Action, Remediation, & Milestones Procedures
- Continuous Monitoring Program (Evidence Artifact)
- Documented Procedure to Run Automated Vulnerability Scanning Tools
- Risk Rating for Remediation Prioritization Diagram
- Vendor-Supplied Security Patching (Evidence Artifact)

6. Related Sub controls

Control Code	Control
3.11.1	Risk Assessment
3.11.2	Vulnerability Scanning
3.11.3	Vulnerability Remediation

7. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition
Vulnerability	An information system or system that is exposed to the possibility of being harmed or accessed without proper authorizations.
Risk	The possibility of monetary or informational loss.
Risk Management	The process of identifying, assessing, evaluating, and managing risks

Vulnerability Scanning	A computer application/program that assesses computers, networks, and applications for known weaknesses.